Position Paper

EBA consultation to the regulatory technical standards on strong customer authentication and secure communication as the key objective of the PSD2

16.12.2015

Federal Association
for Information Technology,
Telecommunications and
New Media

Steffen von Blumröder
Head of
Banking, Financial Services & FinTechs
P +49 30 27576-126
s.vonblumroeder@bitkom.org

Albrechtstraße 10
10117 Berlin
Germany

President
Thorsten Dirks

CEO
Dr. Bernhard Rohleder

Bitkom represents more than 2,300 companies in the digital sector, including 1,500 direct members. With more than 700,000 employees, our members generate a domestic turnover of 140 billion Euros a year, exporting high-tech goods and services worth another 50 billion Euros. They produce hardware and consumer electronics or operate in the sectors of digital media and the network industry. 78 percent of the companies' head-quarters are located in Germany with an additional amount of 9 percent in other countries of the EU and 9 percent in the USA as well as 4 percent in other regions. Bitkom supports an innovative economic policy by focusing the modernization of the education sector and a future-oriented network policy.

Introduction

Bitkom welcomes the opportunity to answer the EBA Discussion Paper on future Regulatory Technical Standards on strong customer authentication and secure communication under PSD 2.

Bitkom believes that the regulatory framework in the European Union provides an adequate environment for business and innovation in the area of e- and m-commerce, including payments. EU legislation on payments, e-money and consumer rights, among others, is among the most advanced globally, and serves as examples for many countries around the world that want to achieve similar market integration, innovation and prosperity. This holds also for the European payments market. We strongly support the initiative to foster a single European market for retail payments and protection of consumer interests. We are certain that the prospect of economic reward is the key driver for innovation.

The pace of development in payments innovation has increased significantly with the development and increasing prevalence of the internet and more recently multi-functional smart phones. The evolution is still ongoing and any final scenario cannot be predicted. Regulatory neutrality must be respected as regards the various types of payment systems and methods. BITKOM therefore insists that any regulatory interference deemed necessary must not disrespect regulatory neutrality.

Consultation questions

Chapter 4.1: Requirements on strong customer authentication

1. With respect to Article 97(1) (c), are there any additional examples of transactions or actions implying a risk of payment fraud or other abuses that would need to be considered for the RTS? If so, please give details and explain the risks involved.

Within banks there is an ongoing Discussion if already the Login Process affords "strong customer authentication" as most of them want to avoid this. It is stated that as long the user cannot change his Master data (or reference data, personal data e.g. like address) **there is no need for a strong customer authentication at the Login**. Please see definition at PSD II §4 (32): "*sensitive payment data' means data, including personalized security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data*;"

Beyond that Bitkom suggests that cases where one of the **payment service providers is located outside the European Union** should be taken into consideration as well, as this could be a fraud factor.

Bitkom believes that any transaction that requires access to confidential data needs to be secured, but we suggest to implement **a leveled approach** that takes the amount and transaction complexity into account. A small amount payment in a retail store should be differently secured than a high value stock trading.

2. Which examples of possession elements do you consider as appropriate to be used in the context of strong customer authentication, must these have a physical form or can they be data? If so, can you provide details on how it can be ensured that these data can only be controlled by the PSU?

Bitkom assumes that regarding the physical element, a personally used device, momentarily smartphone, in future further elements like wearables, watches, cars etc. are the most suited ones. **A smartphone** can be considered the most versatile solution out of following reasons:

- A large existing deployment within customers
- A rich user experience, that may help to improve the information displayed and explained to customers
- A high security implementation using either Software Secure Element (SSE) or Hardware Secure Element (HSE). These components in a Smartphone allow to securely store sensitive data for strong customer authentication
- An evolutive solution based on authentication software downloaded on smartphone
- A solution that may integrate a large range of authentication methods (eg. pin code, fingerprints, voice recognition on data channel, face recognition, handwritten signature)
- A solution that may integrate additional devices based on alternate communication channels like NFC (Nearfield Communication) or BLE (Bluetooth Low Energy)

Regarding the problem of the **smartphone being the payment device and authentication device** at the same time, security and independence can be tackled through a **Software Security Element** for example.

Bitkom believes that a physical form factor can be a limiting element for the PSP (Payment Service Provider) in offering services to a PSU (Payment Service User). A combination of 'What you know' (Knowledge) + 'What you are' (Inherence) removes any technology limitations caused by devices you need to have (Possession). The PSU can control the Data by using tokenization technology and multiple types of data encryption.

In the absence of clarification, Bitkom assumes that **the smartphone is in fact a three possession element** of which two are physical elements, and the third is data: 1) the phone, 2) the SIM and 3) data. In this context the phone and the SIM, the two physical elements, can be used separately. If necessary, the phone can be disabled over the air independently of the SIM. Data is the third possession element on the mobile device, which can be divided into numerous sub-categories in the form of smartphone apps, cloud-based PKI solutions or biometry. All these elements are available to the ecosystem depending on service provider and need.

What is important when deciding **what physical or data elements are appropriate** to be used in the context of strong customer authentication, is to assess the different risks which each solution brings and then to mitigate them in a proportionate way. Data and physical possession elements will be attacked differently with different risks resulting from the security situation. Physical possession elements are relatively secure as the security credentials are stored within the physical device and physical access is needed to get hold of PSCs.

However, independently of the definition of the possession element above, in order to enable a thriving ecosystem of authentication services for consumers, **Bitkom believes that it is key to separate the possession element from the payments service.** Each payment service provider should have the opportunity to use the mobile device as a possession element as long as it is used in an appropriate manner that mitigates the inherent risks of a lost/stolen phone and as long there is a process in place to stop usage when phone is lost/ stolen. According to the Telekommunication providers such processes have already been implemented in mobile phones and in mobile communication networks. A level playing field for authentication services providing strong customer authentication should be ensured independently from PSPs.

Based on the opportunity to use the mobile phone as a tool to enable global consistency, reach and interoperability, we **urge the EBA to ensure that mobile phones can be used as an authentication mechanism** by payment service providers. The mobile phone is the consumer's instrument of choice and should be used for strong customer authentication in an interoperable way with other solutions.

It is important to note that the mobile phone is a two way communication device. The nature of security with a mobile phone is real time and more effective than in current physical payment cards. When the customer calls customer services to notify the loss of the device, the SIM is disabled immediately in real time, which is much more effective than today's capability of physical cards. When a physical payment card is notified as stolen the point of sale device gets updated, but nothing else. Also the mobile device has two physical possession elements that are

separately controlled. The PIN is never stored on the mobile device. There is therefore independence between the factors 'something I have' and 'something I know'.

Bitkom believes that different approaches could be used if the customer accepts them and the usage is in a comfortable way. Therefore also possession elements, like smart cards, key stores, TAN generators could be a possible way depending on the use case. But it is considered imperative that **security must defined as an open standard** in a way that the **user can choose a solution** that fits best to his own needs and that on an open market every manufacturer that is able to produce the hard or software that meets the requirements of the RTS (Regulatory Technical Standards) can offer this products to his customers.

3. Do you consider that in the context of "inherence" elements, behaviour-based characteristics are appropriate to be used in the context of strong customer authentication? If so, can you specify under which conditions?

EBA RTS should specify minimum standards in this area. Key for innovation to take place in this area is that the essential requirements for strong customer authentication are simple and effective. Whilst the **EBA RTS should not pre-empt innovative developments** in this field, they should also not rule out behaviour-based elements and promote them as they can add additional improvement to strong customer authentication. Commercial incentives for innovation need to remain. To offer more sophisticated behaviour-based ways to authenticate users has commercial implications and costs that need to be recouped. It is therefore important that this is left to voluntary commercial agreements.

Users need to have control over their privacy. **Commercial incentives together with users having control over their privacy** are the conditions for more sophisticated behaviour-based authentication services to emerge and to be used by users. One area where inherence elements should be considered, are software-based possession elements. Software-based strong customer authentication solutions could be improved by behaviour-based elements to reach an even better security level for strong customer authentication. Provided these basic conditions are met, inherence based customer authentication will emerge over time and we expect behaviour-based characteristics to become important.

Characteristics etc. should be used in the right context – for example regular transactions are subject to other security arrangements than first-time transactions to new payees. This individual rule-set must be stored at a trusted provider in a secure environment. The categorisation of **"biometrical data" is a subset of personal data** and is defined as "biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability" ("biometric data") by the Article 29 Working Party1. That includes data which is processed by physiological-based and/or behavioural-based techniques2.

[1] The Article 29 Working Party is made up of a representative from the data protection authority of each EU Member State (including the Irish Data Protection Commissioner), the European Data Protection Supervisor and the EU Commission. It acts independently and in a merely advisory capacity. The Working Party publishes opinions and recommendations but does not reflect the opinion of the EU Commission or any other national data protection authority. Due to its membership the Working Party is

Therefore, behavioral elements of an individual person enrolled for example via "keystroke analysis" qualify as biometric data derived from behavioral-based techniques.

Biometrics puts the user and his individuality as centerpiece of security which is or is becoming more and more important and has been an established procedure in crime detection and governmental authentication solutions e.g. eID, border control etc. so that citizens are used to it. In comparison with Factor I and II the third factor "Inherence" is beginning to introduce for the first time the possibility of customer verification as also requested in §4(29) PSD II.

The benefit of biometrics in general is that the factor is always "at hand" (in regular use cases); the benefit of behavioral biometrics in particular is that for verification no extra device is needed.

The discussion about the use of **biometrics cannot be looked at in isolation from privacy law**. Regarding §94 (1) PSD II "Member States shall permit processing of personal data by payment systems and payment service providers when necessary to safeguard the prevention, investigation and detection of payment fraud. ....." and according to 94(2) PSD II "Payment service providers shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user."

As outlined above Biometric data are a subset of personal data, the use of biometric data imposes an obligation to the PSP in fact, but according to our information the use of personal data (here: Biometric data) DOES NOT need explicit consent of the payment service user as mentioned in §94(2) PSD II. This misinterpretation in the PSD II paper needs to be corrected.

As result, despite of the above mentioned limitations, regarding also the results of behavioral biometrics it can be stated that **behaviometrics can be seen as well developed and mature element in the range of biometrics**. Vendors of biometric solutions represent recognition rates between 96 % up to 99 % which are excellent results and that justifies behavioral biometrics as a second factor to ensure strong customer authentication. Since behavior based characteristics are device independent, it ensures that the PSU is always protected regardless of the environment. With the ability to identify friendly fraud easier, and to respond faster in the event of fraud while at the same time providing a better user experience for the PSU behavioral biometrics bears a lot of potential.

4. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to the independence of the authentication elements used (e.g. for mobile devices)?

Bitkom believes that there is **a challenge of user experience and conversion**. Strong customer authentication has to be useful at the specific device /channel. The device specific security characteristics should be part of the specifications. There is not a one fits all solution. Further challenges we perceive are the definition of requirements in a way that the interpretation of the national regulation is limited to a minimum; else this could lead to incompatible solutions and address the largest range of customers that are able to access the service.

close to the data protection authorities and these authorities tend to follow its rather strict recommendations. Nevertheless opinions and recommendations given by the Article 29 Working Party are not binding.
[2] Article 29 WP, WP 193, Opinion 3/12 on developments in biometric technologies, p. 3f.

On the Single-Device topic, the Challenges with independence of authentication elements are already addressed today. Challenges with independence of authentication elements are already known today independently of the smartphone. For example, when a customer loses his payment card, there is a tried and tested process in place that is effective in mitigating the inherent risks. The RTS should therefore build on different procedures that are not limited. Furthermore, the fundamental independence between the mobile device (something the consumer has) and the PIN (something the consumer knows) remains intact even when the mobile device is lost or stolen.

In order to deal with this issue in a forward looking way however, Bitkom believes, EBA should ensure consistency with the approach of e-IDAS Regulation3. E-IDAS has also looked into this issue and come to the following conclusions, which may also be helpful for the EBA to consider. **E-IDASs treats mobile device and business processes as separate elements** and separates the smartphones4 and business processes5 and treats them as separate elements6.

Mobile device and operators' business processes are separate elements. E-IDAS regulation is in line with the mobile operators' view, which also **differentiate between mobile device and the mobile eco-system** (eg.. the mobile device, the mobile network and the mobile operators' business processes) to ensure security. The mobile device is controlled by the consumer whereas SIM security and SIM business processes are always owned by the operator. The element that disappears when a phone is lost/stolen is the device itself. The consumer loses the ability to use the device.

Based on the above, we would suggest that the EBA takes a more differentiated view of the mobile phone, which is a combination of 1) mobile device + 2) mobile business processes + 3) mobile network. With all three of these elements being linked in the mobile phone and actively used, the mobile phone is very secure possession element for payment service users.

5. Which challenges do you identify for fulfilling the objectives of strong customer authentication with respect to dynamic linking?

Bitkom sees the use of dynamic elements and dynamic linking as quite common in standardized authentication/ authorization protocols. It should therefore not impose specific challenges if the generation of response data using cryptographic user credentials (e.g. an electronic signature of dynamic transaction data or an OTP generation based on dynamic transaction data and a user key) is done in a trustworthy environment. For untrusted environments (e.g. a mobile device or a PC/Laptop) dynamic session and/or transaction data may be intercepted and modified by an attacker. It is therefore advisable **to link session and transaction data dynamically to mitigate the risk**.

[3] eIDAS Regulation 910/2014 and e-IDAS Implementing Regulation 2015/1502 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015R1502).
[4] See Art. 2.2. Electronic identification means management' of Commission implementing regulation (EU) 2015/1502
[5] See Art. 2.3. Authentication' of Commission implementing regulation (EU) 2015/1502)
[6] See Article 1.2 of Commission implementing regulation (EU) 2015/1502

With respect to the use of inherence, dynamic linking based on a static physical biometric could be challenging. The inherence should guard against re-use or replay. The **technology for inherence using behavioral biometrics** ensures that the inherence cannot be reused and can be identified as having been used for a specific purpose. Behavioral authentication is linking the behavior of the customer to the entered transaction information. By gathering the behavioral information of the user while entering the transaction, the behavior is correlated to the transaction.

If the behavior of a customer is not matching the stored behavior, a **stepwise authentication could be used**. For low risk transactions this might be omitted, but for high risk transactions this might help preventing fraud. This might be possible by contacting the customer to check if he has really done the transaction in multiple ways, like Two Factor authentication, calling or other means like contacting the customer on a trusted second channel.

The idea of dynamically linking the amount and information on the payee (e.g. parts of the IBAN) can increase security of single payment transactions. Many transactions in Germany combine several credit transfers or direct debits into one payment order. This way a dynamic link to 'the payee' is impossible as there are several payees.

6. In your view, which solutions for mobile devices fulfil both the objective of independence and dynamic linking already today?

A **dedicated mobile application** that implements both, graphic user interface in order to display authentication context (e.g. amount, date, merchant, payment means) and secondly authentication factor that support the graphical user interface to type a pin code & Biometric sensor (Touchdisplay, fingerprint scanner, camera, accelerometer and gyroscope). Cryptographic resources can help to secure exchange with an authentication platform and to create a unique and non-replayable link between authentication and transaction. Hardware or software secure element can be used to support cryptographic features and to give possession characteristic to the device (actually the mobile phone must be specifically personalized for a given end user).

Chapter 4.2: The exemptions to the application of strong customer authentication

7. Do you consider the clarifications suggested regarding the potential exemptions to strong customer authentication, to be useful?

When conceiving the exemptions, EBA must be aware that the strong authentication requirement **can massively influence the retail industry**, e.g. the way and the volume in which consumers purchase goods and services.

EBA should try to facilitate both, customer convenience and security. This cannot be achieved by the strong customer authentication requirement. EBA must allow the payment industry and service & technology providers to **develop modern means of fraud prevention**, which are at the same time customer convenient and sufficiently safe. EBA should allow payment service providers **to deploy alternative means of fraud prevention** (by back-end systems, by behavioral tracking, by any means to be developed in the future) if the payment service provider can demonstrate that such means can achieve the required level of risk avoidance as strong customer authentication.

EBA should extend the **exemption of a transaction risk analysis** to all means of payment (cards, credit transfer, direct debit, e-money).

However, EBA should **not provide small-grained criteria for exemptions**. In its comments, EBA addresses the problem that such analysis must rely on sufficiently detailed information and history from both, the payer and payee. It speaks of real-time risk analysis of the payer's transaction history and the device used for payment and at the same time the detailed risk profile of the payee. The **exemptions should cover certain types of goods and services rather than an individual approach**, looking at each payer and payee separately. Next to this latter method being complicated, it will also be quite costly. Purchases of regular consumer goods and services (books, household articles, food, music, software, tickets, information services, donations to recognised charities) on the internet should be exempted up to a reasonable total price (e.g. €200) per purchase. These transactions are less risky per se, regardless of the individual consumer and shop. The regulator could, as a complementary measure, ask payment service providers to monitor transactions such that certain payers or payees with a conspicuous transaction history can then - in the individual case - be made subject to a strong authentication requirement. Such payers or payees may complain about this more severe and - in their eyes - discriminatory treatment; but these cases can be dealt with on an individual level by the PSPs.

If EBA wishes to maintain **the exemption of white lists**, there should be various **persons to authorize such white lists**. While the consumer is usually not equipped to judge whether a retail shop's payment environment is safe or not, this could be ascertained by professional service providers such as "**Trusted Shop GmbH**" or others. Also, **acquiring payment service providers** could be in a position to ascertain such payment safety of a retail shop.

The EBA recommendation should be in broad terms about the types of capabilities. However, **EBA should refrain from providing details** how they should be implemented or what data should be used. The nature of fraud is that this will evolve rapidly and any detailed recommendations will be obsolete before they are even introduced. **Commercial business considerations** are a very good mechanism to ensure behaviour that prevents risk that would result in financial and reputational losses whilst at a same time providing a commercial incentive to offer innovative commercial.

EBA's RTS should therefore also rely on commercial incentives of the ecosystem to take risk and mitigate it in a responsible manner. This path **ensures innovation and proportionate risk mitigation** whilst at the same time ensuring that consumers can benefit from exemptions, e.g. user-friendly ways of payment. As a rule, **risk-prevention and risk analysis in back-end systems** is almost always preferable to dealing with risk at the consumer interface and making the services more difficult to use for the consumer. One example here is that commercial agreements between the authentication provider and payment service provider may result in a jointly approved confidence score to qualify for an exemption.

At this point it should be stated that the implementation of strong authentication merely caters for the customer log-on security, but does not satisfy the intention of EBA of a user-friendly payment service. For the argument that the risk of logging in is only derived from possible access to sensible payment details, the weighing of risk and security

levels could be drawn on here -alternatively it should be considered to move the security barrier to this point by enabling the access and change of personal data through for example TANs. EBA should unambiguously define the sensible data which require such security measures

8. Are there any other factors the EBA should consider when deciding on the exemptions applicable to the forthcoming regulatory technical standards?

Bitkom believes that a **principle of proportionality** should be taken into consideration. Some exemptions should be added for low risk situations such as **closed loop payments** (tokens with strong usage limitations). Cost of implementing regulatory requirements for some services and exemptions could be disproportionate. We suggest that EBA should provide a list of exemption cases ex ante so that the standardized authentication services can allow for exemptions in their systems. This list should at least cover the exemption cases of PSD2.

Final decision on exemption needs to be done **by payment service provider on a case-by-case basis**. Whilst providers of authentication services provide the necessary data for authenticating the user, the payment service provider needs to make the ultimate risk-assessment on a case-by-case basis with regard to such exemptions, taking into account risks related to the user profile, the use case and fraud potential.

EBA should clarify **which domain is responsible for decision and application of exemptions**: customer's Bank, merchant, merchant's bank, regulator, or scheme? For instance, EBA should clarify what happens when merchant and issuer have different understanding of the exemptions, or risk scoring of transaction. Beyond that it should also be clarified what kind of liability each player takes in case of fraud for exemptions and transactions that require strong authentication or for transactions that does.

9. Are there any other criteria or circumstances which the EBA should consider with respect to transaction risks analysis as a complement or alternative to the criteria identified in paragraph 45?

EBA should extend the exemption of **a transaction risk analysis to all means of payment** (cards, credit transfer, direct debit, e-money).

However, EBA should **not provide small-grained criteria** for exemptions. In its comments, EBA addresses the problem that such analysis must rely on sufficiently detailed information and history from both, the payer and payee. It speaks of real-time risk analysis of the payer's transaction history and the device used for payment and at the same time the detailed risk profile of the payee. The **exemptions should cover certain types of goods and services rather than an individual approach**, looking at each payer and payee separately. Next to this latter method being complicated, it will also be quite costly. Purchases of regular consumer goods and services (books, household articles, food, music, software, tickets, information services, donations to recognised charities) on the internet should be exempted up to a reasonable total price (e.g. €200) per purchase. These transactions are less risky per se, regardless of the individual consumer and shop. The regulator could, as a complementary measure, ask payment service providers to monitor transactions such that certain payers or payees with a conspicuous transaction history can then - in the individual

case - be made subject to a strong authentication requirement. Such payers or payees may complain about this more severe and - in their eyes - discriminatory treatment; but these cases can be dealt with on an individual level by the PSPs.

There are **further criteria to identify a device**, or to be more specific, a browser. For example, there is an approach to identify a browser by means of the installed fonts on the system. Cookies, even if permanently set, are no sufficient criterion in our opinion. The various client side authentication tokens and execution environments provide a different level of trust and security. These different levels are already reflected in various standards and regulations, including the e-IDAS regulation. It should be considered to specify a minimum level of trust for a certain type of transaction and/or to request additional risk management steps if a solution with a low level of trust (e.g. software-based) is used.

Chapter 4.3: The protection of the payment service users'personalised security credentials

10. Do you consider the clarification suggested regarding the protection of users personalized security credentials to be useful?

EBA is concerned that the PSC transmitted via different communications channels (i.e. GSM/GPRS/UMTS, Wifi, NFC and Bluetooth) could be compromised by fraudsters during transmission. Bitkom believes a more differentiated view of transmission channels needs to be adopted. Whilst Wifi and Bluetooth are less secure, the **mobile network** (GSM/GPRS/UMTS/LTE) **is secured** through standard bodies such as 3GPP, which ensure that data transmission is protected by using very strong encryption.

Mobile networks are already regulated by their mobile license conditions, which require strong security to be ensured in the mobile network for communication, storage and processing. SIM and eSIM are not managed from the device operating system, but from the trusted and secure mobile network. Mobile operators are doing independent audits of the network with regard the security of transmission, the network and business processes. The business processes ensure additional security. In addition, mobile operators have strong fraud engines and business processes to complement risk factors arising. No additional regulation is necessary to ensure that these networks are secure. This would therefore involve disproportionate cost and questionable benefit. Regarding NFC payments, the current protocols that support the exchange between the handset and the point of sale include the necessary security for critical data.

EBA is also concerned that the PSC are unwittingly supplied by the user due to social engineering calls, phishing, fraudulent websites, etc. This is no different as to the existing situation with traditional banking services. Similarly, in the mobile network, this can be anticipated through the business process. Once the user makes the call to customer care, the mobile operator can intervene.

EBA requires that all communication channels need to be resistant to tampering and unauthorized access. Bitkom would like to draw attention to the circumstance that the mobile network is in this regard regulated already: **mobile network license conditions require strong security** to be ensured in the mobile network for communication, storage and processing. Mobile operators are doing independent audits of the network with regard to ensure the security of

transmission, the network and business processes. On this basis, we would like the EBA to be mindful of the principle of proportionality: the security measures to protect the confidentiality and the integrity of the consumers' PSC should be proportionate to the risks related to a fraudulent use of the PSCs to carry out fraud or to access sensitive payment data. The mobile network as a whole cannot be changed for the payment activity, which is in comparison to the communication activity miniscule both in terms of activity and revenue.

We recommend altering the clarification text in some parts. E.g. Article 4(31) reads that "**personalized security credentials means personalised features provided by the payment service provider to a payment service user for the purposes of authentication**". Our point of view is that personalized security credentials should not only be provided by the payment service provider. As illustrated in the answers to question 1 and 2 security systems should be described in a way that prevent a situation where the user has to have a complete set of security credentials (knowledge, possession an inheritance) for each of his bank accounts, deposits, accounts with FinTS. In Europe the EBICS standard enables users to reuse their smart cards for different accounts. It is to be challenged, how the log-on token can be protected from unauthorized access to online banking. In this context, the type of software or app which generates and displays the token is relevant, especially since the bank must ensure that no other than the payer can access the token on computers with several users, for example through password encrypted software or app.

11. What other risks with regard to the protection of users' personalised security credentials do you identify?

A risk factor could be the **storing of PSU data** which identifies the PSU. There should be a separation of stored inherence data from the PSU identity such that the compromise of the profile would not risk the identification of the PSU. If credentials are stored in unprotected environments there should be a clear revocation procedure available in case the device is lost or stolen. Since these kinds of devices do not provide any protection against cloning attacks it is recommendable to request measures to mitigate and detect cloning of user credentials. When credentials (or communication involving credentials) are stolen or intercepted there may arise privacy risks due to traceability and likability. The storage and usage of credentials shall therefore be in compliance with existing privacy regulations, e.g. the new European Data Protection regulation.

12. Have you identified innovative solutions for the enrolment process that the EBA should consider which guarantee the confidentiality, integrity and secure transmission (e.g. physical or electronic delivery) of the users' personalised security credentials?

It is recommended to **align the enrolment/provisioning of authentication credentials with existing personalisation processes for payment products/solutions**. In case of hardware tokens (e.g. payment cards) this includes the generation and provisioning of credentials in highly secure and certified environments with end-to-end protection. For mobile channels, Trusted Service Management (TSM) solutions exist that provide a highly secure Over the Air (OTA) provisioning (e.g. as used for SIM/UICC management and subscription management). It is recommended to request similar standards for authentication credentials as well, especially the generation of credentials in a trusted and secure environment, the end-to-end protection during transport/provisioning including strong mutual authentication, and the verification of integrity. For mobile devices it is additionally recommended to issue only

restricted credentials (i.e. with a limited number of transactions and bound to a specific hardware, see question 2) if no hardware supported security environments are available. Beyond that the German banking interface standard (HBCI/FinTs) could enable an enrolment processes by authenticating the PSU with respective to their online banking credentials.

13. Can you identify alternatives to certification or evaluation by third parties of technical components or devices hosting payment solutions, to ensure that communication channels and technical components hosting, providing access to or transmitting the personalized security credential are sufficiently resistant to tampering and unauthorized access?

Bitkom believes that in this context certification is not the best and most efficient tool to solve the problem of tampering and unauthorized access. Even with certification requirements in place there is neither a shift in liability nor in risk of tampering and unauthorized access. Therefore **new technical requirements should be put in in guidelines**. It is better to have a standard that is responsive to events. This would achieve the balance between practicality and combatting fraud. In an environment where all elements/components are certified already this might be a quicker and more effective response than certification. We therefore don't see any need for certification to solve the problem of fraud.

14. Can you indicate the segment of the payment chain in which risks to the confidentiality, integrity of users' personalised security credentials are most likely to occur at present and in the foreseeable future?

The highest risks are to be expected for **remote communication use cases** (e.g. online payment) via insecure channels. Most issues can be expected on the client side when users can be subject to social engineering and phishing attacks. It is therefore recommendable to request appropriate device/ token security with high tamper resistance as well as protocols that are resistant to phishing and, man-in-the-middle attacks. If user credentials are stored on the server side or generated for one-time use (e.g. with tokenisation) then the server shall provide sufficient security as well. **End-to-end protection is recommended** for enrolment/provisioning as well as for the token/client device/server communication chain.

Chapter 4.4: Considerations prior to developing the requirements on common and secure open standards of communication

15. For each of the topics identified under paragraph 63 above (a to f), do you consider the clarifications provided to be comprehensive and suitable? If not, why not?

a. EBA has to define **technical protocols for such standard** (e.g. OAuth2 for authentication or REST/JSON web services for communication). Not to forget there are 4 needs to cover: identification, authentication, notification, and information.

b. In this context, the **TPP needs to be identified with a license number** given by local regulators or by EBA through the general directory it will manage. Such license number could be the LEI or any other identifying number.

c. In the PSD2 text, **payees are included in the loop** and not only PIS/AIS/ASPSP are concerned by the common and open standards for communication.

d. **Need for information about payment history** for audit track for instance. About account information communicated by ASPSPs, indicate which data are mandatory or optional and which are sensitive and not in view of the future regulation of personal data protection. Indeed in PSD2, we can read that IBAN and name are not sensitive.

f. in the text, it is **too restrictive to try to define ASPSP interface** because ASPSP can use a distinct provider to avoid any IT development in internal and use a converter of protocol for any communication with new PIS/AIS.

16. For each agreed clarification suggested above on which you agree, what should they contain in your view in order to achieve an appropriate balance between harmonisation, innovation while preventing too divergent practical implementations by ASPSPs of the future requirements?

They should contain **a minimum standard for specific information processes**, which are needed to identify and logon the user against the ASPSs in case of AIS and PIS usage. We can imagine that protocol could be different for a PIS and a AIS from a risk point of view. Indeed PIS will debit the account whereas the AIS will only consolidate banking information. The timing for future implementation of API by ASPSP will be short: in consequence a minimum set of practices commonly approved by banks' industry should be integrated. Besides, PSD2 mentions account accessible online: but online could be in cloud or through connected object.

17. In your opinion, is there any standards (existing or in development) outlining aspects that could be common and open, which would be especially suitable for the purpose of ensuring secure communications as well as for the appropriate identification of PSPs taking into consideration the privacy dimension?

The recently published **e-IDAS specification 1.0 together with the e-IDAS token specification BSI /ANSSI TR 03110** as respective profile containing the use of tamper resistant user token for storage and use of secure user credentials reflect as well privacy requirements in a suitable and comprehensive way. Therefore, this standard could be valuated as an appropriate standard for eID management, secure communication and strong authentication with very high security level. A profile including implementations for Secure Elements (SE) is the **EN 419212 standard for SE** used as qualified signature/ seal creation devices would additionally be appropriate for web authentication, secure communication and confidentiality services with very high level of assurance. In addition, the **FIDO protocol** offers a strong and privacy friendly authentication with context specific suitable security level which can be also combined with federation protocols (e.g. SAML, OpenID Connect). For SIM-based mobile devices **the GSMA Mobile Connect protocol** also offers strong authentication with context specific suitable security level.

Other relevant standards would include the **Global Platform Secure Channel Protocol, EMVCo Next Gen including privacy protocol, and ISO 12812 Mobile Payment**. Beyond that the infrastructure of some of the TPPs, which

combines different standards (e.g. HBCI/FinTS) and common bank APIs and make them extremely easy to use for third parties, is a good example. PSP could be identified through a number of identification supplied by each local regulator and centralized by EAB in its directory listing all the PIS and AIS. Nevertheless services 7&8 identified in annexe I of PSD2 can be proposed by any others categories of PSP listed in article I (1). So identification is not only PIS/AIS : EBA register should be also available both per services and per categories of PSP.

18. How would these requirement for common and open standards need to be designed and maintained to ensure that these are able to securely integrate other innovative business models than the one explicitly mentioned under article 66 and 67 (e.g. issuing of own credentials by the AIS/PIS)?

If we consider the **banking account as a commodity** independent from any ASPSP, it means that the account could be accessible by any methods of authentication. User could be the decision maker concerning the credentials to sue through a dashboard attached to a new service "I manage my credentials" for instance.

Besides if AIS/PIS identify themselves for each communication session, it could be dangerous because a switch from AIS to PIS is possible on a same communication session and the service is different. So we would suggest **identification of TPP for activation of each service**.

Open standards could ensure other innovative business models and solutions and can enhance existing ones. They have to comply with other regulations and directives in Europe **as e-IDAS and the Data Protection Regulation** and therefore could face new requirements. As an example, the storage and usage of credentials shall be in compliance with existing privacy regulations, e.g. the new European Data Protection regulation. The requirements should be **designed and maintained openly** (access to everyone), in a **flexible and scalable way** (depending on the risk of the credentials / assets to be protected) and cover different technical implementations. They should be **reviewed on a regular basis** to support new technologies as well as new attack scenarios.

Chapter 4.5: Possible synergies with the regulation on electronic identification and trust services for electronic transactions in the internal market (e-IDAS)

19. Do you agree that the e-IDAS regulation could be considered as a possible solution for facilitating the strong customer authentication, protecting the confidentiality and the integrity of the payment service users' personalised security credentials as well as for common and secure open standards of communication for the purpose of identification, DP on future RTS on strong customer and secure communication under PSD2 31 authentication, notification, and information? If yes, please explain how. If no, please explain why.

Yes, Bitkom agrees with respect to the e-ID, customer authentication, and secure communication the related standards could be used for PSD2 as well regarding the addressed matters. Yet, regarding the requirement "confidentiality" of communication there is no direct reference inside the e-IDAS regulation, but only in an implicit way referring to privacy in general which does actually imply a confidential transfer of communication.

20. Do you think in particular that the use of "qualified trust services" under e-IDAS regulation could address the risks related to the confidentiality, integrity and availability of PSCs between AIS, PIS providers and ASPSPs? If yes, please identify which services and explain how. If no, please explain why.

As mentioned above, together with the referred generic privacy requirement, the qualified trust services, especially the seal services, are described very explicitly fulfilling data originality and data integrity to be applied for legal persons as e.g. AIS, PIS and ASPSDs. The gain of this new concept is that qualified seals are accepted as such European–wide and cannot be interpreted differently as it was the case with qualified signatures before, as substitute for "handwritten signatures".